Zscaler Zero Trust Firewall

Protection Zero Trust sécurisée et adaptative du trafic web et non web. 100 % cloud-native.

FICHE TECHNIQUE

Zscaler Zero Trust Firewall protège le trafic web et non web pour tous les utilisateurs, toutes les applications et tous les sites grâce à la plateforme SSE (Security Service Edge) cloud native la plus complète du secteur.

Le monde du travail est désormais disséminé et mobile. Les applications migrent des data centers vers le cloud, tandis que les nouvelles charges de travail digitales sont de plus en plus déployées nativement dans le cloud. En outre, les utilisateurs qui travaillent depuis différents emplacements, notamment en télétravail, dans les espaces de travail partagés, les filiales et à distance, accèdent aux applications professionnelles directement depuis Internet.

En conséquence, les utilisateurs et les applications cloud génèrent des volumes de trafic élevés qui sont backhaulés vers des appliances de sécurité traditionnelles centrées sur le réseau, ce qui a un impact sur la productivité et crée une congestion de la connectivité tout en ajoutant des risques pour l'entreprise. Sans inspection complète du trafic chiffré par SSL, les adversaires utilisent le chiffrement et les ports non standard pour échapper à la détection et mener des attaques furtives. Les pare-feu virtualisés tentent de remédier à la situation, mais ils sont conçus pour étendre votre réseau aux ressources cloud et présentent les mêmes limitations de capacité.

Pour garantir l'interconnectivité et sécuriser les charges de travail, vous aurez toujours besoin de ressources dédiées pour administrer correctement sous peine d'erreurs de configuration.

Zscaler Zero Trust Firewall

Zscaler Zero Trust Firewall offre une protection basée sur le cloud pour le trafic Web (HTTP/HTTPS) et le trafic non Web (FTP, DNS, RDP, Telnet et plus) pour tous les utilisateurs et appareils, quel que soit l'endroit où ils se connectent. Il améliore la connectivité et la disponibilité en dirigeant le trafic de manière sécurisée à l'aide de points d'accès locaux à Internet, sans backhauling via des VPN et sans dupliquer la pile d'appliances de sécurité sur chaque site. En acheminant les connexions Internet et SaaS vers Zscaler, il garantit l'inspection de l'ensemble du trafic utilisateur, y compris le trafic chiffré SSL, en s'adaptant de manière élastique pour gérer des volumes élevés de connexions de longue durée.

Zero Trust Firewall aide les entreprises à respecter les normes réglementaires tout en configurant, gérant et appliquant de manière universelle une protection contre les menaces adaptée aux utilisateurs et aux applications, ainsi que des politiques basées sur les risques, afin de garantir la visibilité sur le réseau et les applications à l'aide d'une console centralisée de gestion des politiques. Étant donné qu'il s'agit d'une solution de pare-feu en tant que service (FWaaS), la responsabilité des mises à jour, des mises à niveau et des correctifs, y compris les exigences en matière d'évolutivité, incombe à Zscaler. Cela peut permettre de réaliser d'importantes économies en remplaçant les appliances et supprime les matrices complexes de politiques et de configurations réseau liées à des emplacements physiques.

Zscaler Zero Trust Firewall enregistre chaque session afin de fournir une visibilité sur l'ensemble des utilisateurs et des emplacements, ce qui vous garantit l'accès aux informations dont vous avez besoin, exactement au moment où vous en avez besoin. En transformant vos connexions hybrides et de sites distants, et en répondant dès aujourd'hui aux besoins en matière de sécurité et de performance, Zscaler prend en charge et évolue pour répondre à vos besoins de transformation vers le cloud, notamment la migration vers des applications cloud natives telles que Microsoft 365.

AVANTAGES DE ZSCALER ZERO TRUST FIREWALL :

- **Protection complète pour les utilisateurs en télétravail.** Des politiques de sécurité dynamiques basées sur les risques suivent vos utilisateurs à chaque connexion, sans matrice complexe de politiques et de configurations réseau.

- **Inspection complète pour détecter les attaques cachées.** L'inspection illimitée du trafic en mode inline et le déchiffrement SSL natif empêchent les menaces furtives et clôturent les connexions malveillantes.

- **Détection du trafic web furtif sur les ports non standard.** Identifiez et interceptez rapidement les cybermenaces furtives et chiffrées utilisant des ports non standard.

- **Points d'accès locaux à Internet fournis dans le cloud.** Des connexions Internet directes, rapides et sécurisées pour tout le trafic hybride et des sites distants évoluent de manière élastique et améliorent l'expérience utilisateur.

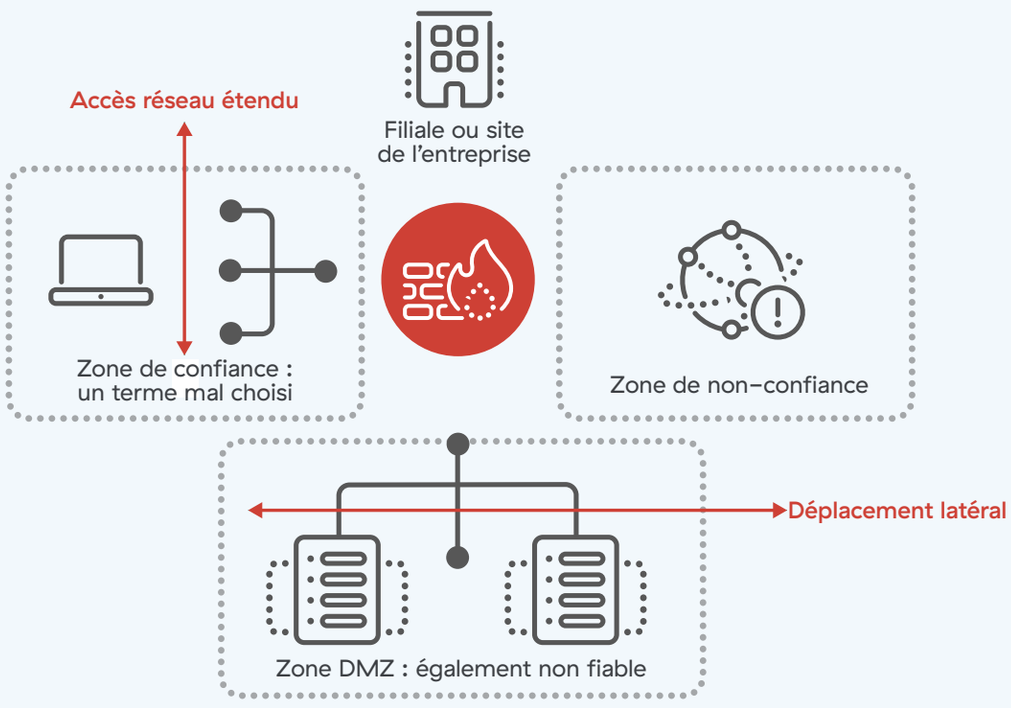
- **Système de prévention des intrusions (IPS) cloud toujours actif.** Les signatures IPS comportementales adaptatives, gérées par Zscaler ThreatLabz, fonctionnent en temps réel pour enrichir les workflows SecOps.

- **Sécurisation du DNS sans compromission des performances.** Les résolutions localisées garantissent des performances supérieures, tout en protégeant vos utilisateurs et vos terminaux des sites malveillants et du tunneling DNS.

- **Protection fournie dans le cloud avec une présence mondiale en périphérie.** Zscaler Zero Trust Firewall fournit une sécurité et une expérience utilisateur inégalées, entièrement intégrées à Zscaler Internet Access™ et faisant partie de Zscaler Zero Trust Exchange™.

Dépasser l'architecture traditionnelle avec Zscaler Zero Trust Firewall

Pare-feu traditionnel – Architecture basée sur la zone



Plateforme Zero Trust de Zscaler

Les pare-feux traditionnels et les pare-feux de nouvelle génération ne sont pas en mesure de satisfaire les exigences de Zero Trust de la norme NIST 800-207. L'architecture de sécurité basée sur le périmètre n'a pas été conçue pour inspecter le trafic chiffré à grande échelle sur des réseaux et des appareils non protégés. L'absence d'authentification stricte des utilisateurs et de contrôles continus des politiques à chaque étape peut entraîner la compromission d'un serveur ou d'un appareil et accorder aux hackers un large accès au réseau et la possibilité d'effectuer des déplacements latéraux non autorisés. En outre, l'utilisation d'un pare-feu traditionnel comme passerelle pour déployer un réseau privé virtuel (VPN) expose vos réseaux publics et privés. Seul un pare-feu Zero Trust peut offrir un accès dynamique et basé sur le moindre privilège pour piloter la transformation du réseau et de la sécurité.

Avantages d'un pare-feu cloud natif

Spécialement conçu pour le monde numérique actuel, Zscaler Zero Trust Firewall vous garantit un accès sécurisé à Internet et la prise en charge de l'ensemble du trafic web et non web, sur tous les ports et protocoles, avec une évolutivité et des performances optimales. Vos utilisateurs bénéficient d'une protection cohérente quel que soit l'appareil qu'ils utilisent ou leur emplacement (en télétravail, au siège ou dans les filiales, ou en déplacement) sans les limitations liées au coût, à la complexité et aux performances de la sécurité réseau traditionnelle et des appliances de pare-feu de nouvelle génération.

SOLUTION OPTIMISÉE PAR UNE PLATE-FORME ZERO TRUST ADAPTATIVE

Ne faites plus de compromis sur les inspections statiques, la dégradation des performances et les limites de capacité des appliances de pare-feu physiques. Basé sur une plateforme cloud native entièrement intégrée, Zscaler Zero Trust Firewall évolue de manière élastique pour gérer le trafic des applications cloud nécessitant des connexions pérennes, tout en interceptant et inspectant nativement le trafic SSL/TLS, à grande échelle, afin de détecter les malwares dissimulés dans le trafic chiffré.

CONNEXIONS HYBRIDES ET CONNEXIONS AUX FILIALES TRANSFORMATRICES

Passez d'une infrastructure coûteuse et centrée sur le réseau à de véritables points d'accès locaux à Internet fournis dans le cloud. Acheminez le trafic Internet en local afin de fournir des connexions directes et rapides vers le cloud, tout en assurant la sécurité et le contrôle d'accès sur tous les ports et à tous les protocoles. Ne nécessitant pas le déploiement ni la gestion d'appliances, cette solution réduit les coûts de backhauling MPLS et élimine la gestion coûteuse et fastidieuse des correctifs, la coordination des fenêtres d'interruption de service et la gestion des politiques.

UNE SÉCURITÉ OMNIPRÉSENTE POUR DES EFFECTIFS MODERNES

Tirez parti des mises à jour de sécurité en temps réel, informées par 300 000 milliards de signaux quotidiens et partagées chaque jour sur l'ensemble du cloud, pour une protection identique sur tous les appareils, quel que soit l'endroit où les utilisateurs se connectent. En rapprochant l'ensemble de la pile de sécurité de l'utilisateur, celui-ci bénéficie d'une protection inégalée contre les menaces liées à l'utilisateur et aux applications, grâce à des politiques dynamiques de suivi sur le réseau de l'entreprise et en dehors de celui-ci.

BLOCAGE PERMANENT DES ATTAQUES MALVEILLANTES CONNUES

Franchissez les limites des solutions traditionnelles grâce à la protection contre les menaces du système de prévention des intrusions (IPS) fournie dans le cloud, adaptée au contexte et gérée par Zscaler ThreatLabz. Grâce à l'inspection illimitée et inline du trafic, y compris le trafic IOT/OT et chiffré sur le réseau et en dehors de celui-ci, les signatures IPS comportementales sont appliquées en temps réel lors de l'accès à des milliers d'applications web et non web, quel que soit le type de connexion ou l'emplacement.

OPTIMISEZ LE DNS POUR LA PERFORMANCE ET LA SÉCURITÉ

Accélérez la résolution des problèmes en associant des applications géographiquement proches, améliorant ainsi l'expérience utilisateur et les performances des applications cloud, tout en mettant en œuvre des politiques de sécurité et de contrôle du système de noms de domaine (DNS). Grâce à l'inspection SSL à grande échelle, regagnez en visibilité et empêchez les hackers d'abuser du DNS-over-HTTPS (DoH), protégeant ainsi mieux les utilisateurs et les employés contre l'accès aux domaines malveillants et le contournement des politiques de l'entreprise. En fournissant un service DNS, Zscaler minimise la latence et sécurise les points d'accès locaux à Internet à l'aide de proxy traitant tout le trafic DNS, et s'appuie sur l'apprentissage automatique pour détecter et neutraliser les potentiels tunnels d'exfiltration de données.

GESTION DES POLITIQUES FACILE À COMPRENDRE

Définissez, déployez et appliquez immédiatement des politiques universelles pour tous les utilisateurs, sur tous les sites, à partir d'une console unique. En lieu et place des matrices complexes de politiques, des configurations réseau et de la recréation de politiques pour chaque emplacement des pare-feu classiques, Zero Trust Firewall simplifie la gestion des politiques en centralisant les règles granulaires de pare-feu en fonction de l'utilisateur, de l'application, de l'emplacement, du groupe et du service. De plus, les administrateurs peuvent envoyer des journaux complets enrichis des détails de l'utilisateur, des demandes, des réponses, des services utilisés, etc., aux outils SIEM et XDR afin d'améliorer les enquêtes de sécurité et la réponse aux incidents.

Gartner

Zscaler, désigné leader du MQ SSE de Gartner, obtient le meilleur positionnement sur le critère de la « capacité d'exécution ».

EN SAVOIR PLUS →

Principales caractéristiques de Zscaler Zero Trust Firewall

Gestion centralisée des politiques	Définissez et appliquez immédiatement les politiques sur tous les sites sans avoir à recréer des politiques pour chaque site.
Services de sécurité entièrement intégrés	Les informations contextuelles sont partagées entre les services DLP, APT, sandbox et autres pour offrir une meilleure protection et une plus grande visibilité.
Contrôle granulaire, journalisation et visibilité en temps réel	Une journalisation enrichie pour une visibilité détaillée, avec une journalisation unifiée au niveau mondial et illimitée pendant six mois, permettant l'analyse et la corrélation pour dégager des tendances, analyser la productivité et résoudre les problèmes.
Protection contre les menaces en fonction de l'utilisateur	Définissez les utilisateurs par groupes, départements ou sites, notamment en définissant le télétravail ou les utilisateurs distants en tant qu'emplacement, et intégrez les fournisseurs d'identité et les bases de données d'utilisateurs locaux, ce qui permet d'appliquer des politiques cohérentes quel que soit l'emplacement physique des utilisateurs.

Principales caractéristiques de Zscaler Zero Trust Firewall (suite)

Protection contre les menaces en fonction des applications	Identifiez et classez les services applicatifs dès le premier paquet pour activer les politiques de filtrage et de transfert du pare-feu, en prenant des mesures immédiates et de plus haute priorité avec des politiques adaptatives et contextuelles. Prise en charge des types d'applications dans tous les services réseau : ports et protocoles, applications réseau ; SNI (nom d'hôte), services basés sur le DPI, services applicatifs ; UCaaS basés sur l'identification du premier paquet, IP, groupes FQDN et autres détections basées sur l'heuristique.
Sécurité et contrôle IPS adaptatifs	Protection permanente contre les menaces dans le cloud grâce à des signatures IPS personnalisées et à des milliers de signatures IPS adaptatives et comportementales sur tous les ports et protocoles, quel que soit le type de connexion ou l'emplacement, en inspectant l'ensemble du trafic Internet de l'utilisateur. Consultez la liste de toutes les signatures IPS gérées par ThreatLabZ.
Inspection de sécurité avancée	Effectuez une inspection complète des paquets sur les protocoles non Web, notamment FTP, DNS, RDP, Telnet, etc. pour identifier et empêcher le trafic évasif sur les ports non standard.

Principales caractéristiques de Zscaler Zero Trust Firewall (suite)

Sécurité et contrôle DNS	Optimisez les performances des applications cloud et minimisez la latence tout en garantissant une sécurité sans compromission en faisant passer tous les DNS par Zscaler. Activez des politiques basées sur l'utilisateur, l'application, l'emplacement et le pays de l'IP résolue pour bloquer automatiquement les utilisateurs provenant de domaines malveillants, et pour détecter et empêcher le DNS tunneling. • **Résolution :** le DNS-as-a-service offre une résolution optimale avec localisation, gestion des locataires et latence minimale • **Filtrage DNS :** créez des règles de filtrage DNS personnalisées pour bloquer, autoriser ou rediriger différents types de requêtes DNS vers des destinations connues et malveillantes • **Sécurité et exfiltration de données :** détectez les logiciels malveillants, l'hameçonnage, le DNS tunneling et l'exfiltration de données à l'aide de l'apprentissage automatique. • **DNS over HTTPS (DoH) :** évitez les angles morts DoH et le contournement des contrôles organisationnels lors du chiffrement des connexions DNS dans le trafic HTTPS courant
Politiques relatives aux noms de domaine pleinement qualifiés (FQDN)	Configurez et gérez facilement les politiques d'accès pour les applications hébergées sur plusieurs adresses IP.
Contrôle du protocole de transfert de fichiers (FTP) et prise en charge du NAT (Network Address Translation)	Prise en charge du contrôle d'accès FTP et FTP over HTTP et prise en charge du proxy de destination NAT et de la redirection NAT
Certifications de confidentialité et de conformité	Conformité aux normes internationales les plus strictes en matière de risques et de confidentialité, applicables aux entreprises et aux organisations publiques
Conformité aux réglementations sectorielles et de confidentialité des données	Conformité aux réglementations sectorielles et nationales en matière de confidentialité des données
Protection mondiale partagée	Bénéficiez de l'effet cloud : chaque fois qu'une nouvelle menace est identifiée dans une des dizaines de milliards de transactions traitées quotidiennement par Zscaler Cloud, tous les utilisateurs de Zscaler, où qu'ils soient, en sont protégés.

Composante entièrement intégrée de Zscaler Internet Access, Zscaler Zero Trust Firewall est inclus dans les éditions ZIA et Zscaler for Users Essentials et Business. Les fonctions avancées de Zscaler Zero Trust Firewall sont incluses dans les éditions ZIA et Zscaler for Users Transformation et Unlimited, ainsi que dans un module complémentaire des éditions Essentials et Business.

	Standard	Advanced
CRITÈRES DE POLITIQUE DE ZERO TRUST FIREWALL		
Services de réseau et d'application	✓ Jusqu'à 10 règles	✓
Vérification du filtrage FQDN		✓
Connaissance de l'emplacement		✓
Sensibilisation des utilisateurs — vérification	–	✓
Application réseau (DPI)	–	✓
Politique dynamique basée sur le risque	–	✓
Règles de pare-feu	✓ Jusqu'à 10 règles	✓ Jusqu'à plus de 1 000 règles
CONTRÔLE DNS		
Trusted Resolver pour la résolution DNS	✓	✓
Filtrage et sécurité DNS	✓ Jusqu'à 64 règles	✓
Détection des tunnels DNS et des applications	–	✓
CONTRÔLERAI IPS	–	✓
CONTRÔLE DU FTP	✓	✓
CONTRÔLE NAT	✓	✓

FONCTIONNALITÉS DE LA PLATEFORME		
Inspection SSL complète	✓	✓
Journalisation en temps réel	✓ Détails de la journalisation agrégée pour les actions d'autorisation du pare-feu et détails de la journalisation détaillée pour les actions de blocage avec des journaux DNS complets. **Inclus dans les licences Essentials et Platform**	✓ Tous les journaux pour toutes les actions et toutes les fonctions, y compris l'ID de l'utilisateur, l'ID de l'application, l'IPS, etc. **Licence additionnelle requise**

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange™, basé sur le SSE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

+1 408 533 0288 **Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/fr**

zscaler™

Zero Trust Everywhere